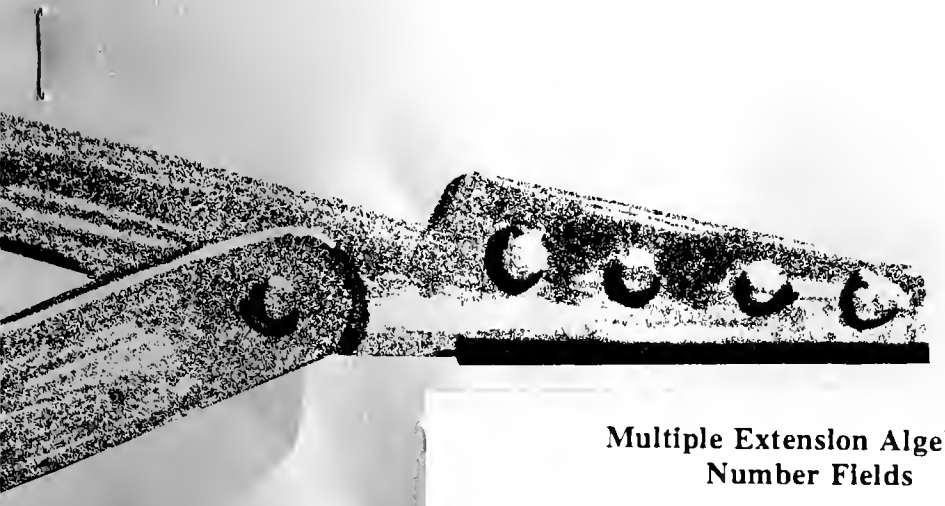
Robotics Research Technical Report



Multiple Extension Algebraic Number Fields

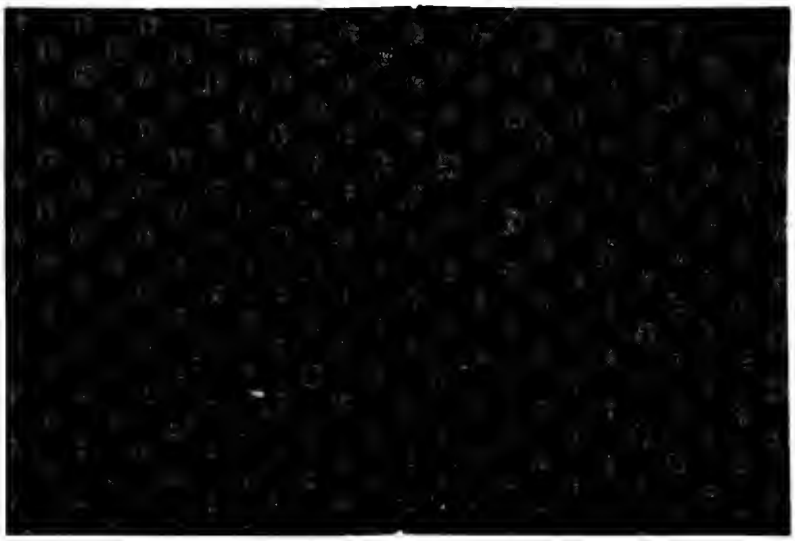
by

Chung-jen Ho

Technical Report No. 432
Robotics Report No. 190
March, 1989

New York University
Courant Institute of Mathematical Sciences

Computer Science Division
251 Mercer Street New York, N.Y. 10012



Multiple Extension Algebraic Number Fields

by

Chung-jen Ho

Technical Report No. 432
Robotics Report No. 190
March, 1989

New York University
Dept. of Computer Science
Courant Institute of Mathematical Sciences
251 Mercer Street
New York, New York 10012

Work on this paper has been supported by National Science Foundation Grant CCR-8703458.

Abstract

Let α be an algebraic integer satisfying a monic irreducible polynomial $A(t) \in \mathbf{Z}[t]$. The algebraic integers contained in $\mathbf{Q}(\alpha)$ form a ring which we shall denote by $\mathcal{R}_\alpha$. It is known that if $C_\alpha = \mathrm{disc}(A)$ then $\mathcal{R}_\alpha \subseteq \frac{1}{C_\alpha}\mathbf{Z}[\alpha]$, where $\mathrm{disc}(A)$ is the *discriminant* of A. Let β be a root of a prescribed monic irreducible polynomial $B(u) \in \mathbf{Z}[\alpha][u]$. Let the algebraic number field $\mathbf{Q}(\alpha)(\beta)$ be given as the field $\mathbf{Q}(\alpha)$ extended by β. We denote by $\mathcal{R}_{\alpha\beta}$ the algebraic integers contained in $\mathbf{Q}(\alpha)(\beta)$. In this paper, we present an algorithm to compute an integer C_β such that

$$\mathcal{R}_{\alpha\beta} \subseteq \frac{1}{C_\alpha C_\beta}\mathbf{Z}[\alpha][\beta].$$

The algorithm takes $O(\delta_B^3 \delta_A \log \delta_A + \delta_A^3)$ arithmetic operations where δ_A and δ_B are the degree of A and B respectively. With this result, we generalize the Lenstra's algorithm [6] for factoring polynomials over algebraic number field. Our algorithm computes the factorization of univariate polynomials over algebraic number field $\mathbf{Q}(\rho_1)(\rho_2)\cdots(\rho_z)$ where ρ_j $(j = 1, \ldots, z)$ is recursively defined as follows: ρ_1 is an algebraic number and ρ_j is algebraic of degree ≥ 2 over $\mathbf{Q}(\rho_1)(\rho_2)\cdots(\rho_{j-1})$. The number of arithmetic operation and the binary length of integers required by this algorithm are polynomial in the degree and the LOG of the coefficients of input polynomials.

1 Introduction

Throughout this paper, we denote by δ_F the degree of an univariate polynomial F. For any polynomial $F = \sum_{i=0}^{\delta_F} c_i x^i \in \mathbf{Z}[x]$, we denote by $\|F\|_2$ the value of $\sqrt{\sum_{i=0}^{\delta_F} c_i^2}$ and by $F_{\max}$ the value of $\mathbf{max}\{c_0, c_1, \ldots, c_{\delta_F}\}$. Let α be an algebraic integer satisfying a monic irreducible polynomial $A(t) \in \mathbf{Z}[t]$. The algebraic integers contained in $\mathbf{Q}(\alpha)$ form a ring which we shall denote by $\mathcal{R}_\alpha$. It is known that if $C_\alpha = \mathbf{disc}(A)$ then $\mathcal{R}_\alpha \subseteq \frac{1}{C_\alpha}\mathbf{Z}[\alpha]$, where $\mathbf{disc}(A)$ is the *discriminant* of A. Let β be a root of a prescribed monic irreducible polynomial $B(u) \in \mathbf{Z}[\alpha][u]$. Then β is an algebraic integer (see [3]). Thus, $\mathbf{Z}[\alpha][\beta]$ is a domain of algebraic integers (see [5]). Let the algebraic number field $\mathbf{Q}(\alpha)(\beta)$ be given as the field $\mathbf{Q}(\alpha)$ extended by β. We denote by $\mathcal{R}_{\alpha\beta}$ the algebraic integers contained in $\mathbf{Q}(\alpha)(\beta)$. Clearly, $\mathcal{R}_{\alpha\beta}$ is a ring and $\mathbf{Z}[\alpha][\beta] \subseteq \mathcal{R}_{\alpha\beta}$. Our problem is to find an integer C_β such that

$$\mathcal{R}_{\alpha\beta} \subseteq \frac{1}{C_\alpha C_\beta}\mathbf{Z}[\alpha][\beta]. \tag{1}$$

In fact, we can translate a double extension to a simple extension and then compute a discriminant to get an integer $C_{\alpha\beta}$ such that $\mathcal{R}_{\alpha\beta} \subseteq \frac{1}{C_{\alpha\beta}}\mathbf{Z}[\alpha][\beta]$. However, this method takes arithmetic operations $O(\delta_A^6\delta_B^3)$. We call this method the naive algorithm. In this paper, we present an algorithm to compute the C_β. It only takes $O(\delta_B^3\delta_A \log \delta_A + \delta_A^3)$ arithmetic operations. Furthermore, the integer $C_{\alpha\beta}$ produced by the naive algorithm has binary length

$$O(\delta_A^4\delta_B^2 + (\delta_A^3\delta_B^2 + \delta_A^4\delta_B)\log A_{\max} + \delta_A^4\delta_B \log B_{\max}).$$

But, the integer $C_\alpha C_\beta$ produced by our algorithm has binary length

$$O(\delta_A\delta_B(\log \delta_B + \delta_A \log A_{\max} + \log B_{\max})).$$

Therefore, our algorithm is much better than the naive algorithm. Note that we haven't defined $B_{\max}$. $B_{\max}$ is defined as follows:

Definition If $B(u) = \sum_{j=0}^{\delta_B}\sum_{i=0}^{\delta_A-1} b_{ij}\alpha^i u^j$, then $B_{\max} = \mathbf{max}\{b_{ij}; 0 \le i < \delta_A, 0 \le j \le \delta_B\}$.

The following typed variables will be used:

1. $\alpha, \beta, \sigma, \zeta, \varepsilon, \Delta, \Upsilon, \Gamma, \Psi$ are algebraic integers.

2. $a, b, c, d, e, i, j, k, l, m, n, w$ and $C_\alpha, C_\beta, C_\sigma$, are integers.

3. $\mathcal{R}_\alpha, \mathcal{R}_{\alpha\beta}, \mathcal{R}_{\sigma_1 \cdots \sigma_j}$ are domains of algebraic integers.

4. A, B, E, F, G are univariate polynomials over algebraic integer domains.

5. D, K, N are integers.

6. L is a lattice.

In Section 2, we briefly describe the naive algorithm and analyze it. Section 3 contains the main result of this paper. In Section 4, we extend our result to the algebraic number field $\mathbf{Q}(\sigma_1)(\sigma_2)\cdots(\sigma_z)$, where σ_j $(j = 1, \ldots, z)$ are recursively defined as follows:

$$\begin{cases} \sigma_1 \text{ is an algebraic integer} \\ \sigma_j \text{ is integral of degree} \geq 2 \text{ over } \mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_{j-1}]. \end{cases} \tag{2}$$

With this result, we generalize the Lenstra's algorithm [6] for factoring polynomials over algebraic number field. Our algorithm computes the factorization of monic squarefree polynomials over algebraic number field $\mathbf{Q}(\sigma_1)(\sigma_2)\cdots(\sigma_z)$. The number of arithmetic operation and the binary length of integers required by this algorithm are polynomial in the degree and the LOG of the coefficients of input polynomials. Of course, our algorithm is better than the naive algorithm by translating a multiple extension to a simple extension and then factoring over the simple algebraic extension of the rational number field.

2 The Naive Algorithm

Let $A, B, \alpha, \beta, \mathcal{R}_\alpha$ be as in section 1. The following is a well known result.

Lemma 1 *If* $C_\alpha = \mathbf{disc}(A)$, *then* $\mathcal{R}_\alpha \subseteq \frac{1}{C_\alpha}\mathbf{Z}[\alpha]$.

In the naive algorithm, we first compute an integral polynomial $\hat{B}(u) \in \mathbf{Z}[u]$ such that β is a root of $\hat{B}(u)$. Let $B(t,u)$ be a bivariate polynomial obtained by replacing α in $B(u)$ by t. Thus $B(t,u) \in \mathbf{Z}[t][u]$. By [3, page 185], we can take $\hat{B}(u) = \mathbf{res}_t(A(t), B(t,u))$ where $\mathbf{res}_t(A,B)$ denotes the *resultant* of A and B with respect to t. Then, compute a bivariate polynomial $G(t,y) = \mathbf{res}_u(A(t-yu), \hat{B}(u))$; and then compute an integer y_0 such that $\mathbf{disc}(G(t,y_0)) \neq 0$. From Loos [3, page 185], $G(t,y_0)$ has a root $\gamma = \alpha + y_0\beta$ and $\mathbf{Q}(\gamma) = \mathbf{Q}(\alpha)(\beta)$. If we let $C_{\alpha\beta} = \mathbf{disc}(G(t,y_0))$, then clearly, by Lemma 1, we have $\mathcal{R}_{\alpha\beta} \subseteq \frac{1}{C_{\alpha\beta}}\mathbf{Z}[\gamma] \subseteq \frac{1}{C_{\alpha\beta}}\mathbf{Z}[\alpha][\beta]$.

Because $\hat{B}(u)$ has degree $\delta_A\delta_B$, the bivariate polynomial $G(t,y)$ has degree $\delta_A^2\delta_B$ with respect to variable t or variable y. Thus, it takes $O(\delta_A^6\delta_B^3)$ arithmetic operations to compute $\mathrm{disc}(G(t,y_0))$. When regarding $G(t,y)$ as a polynomial in t over $\mathbf{Z}[y]$, let $F(y) = \mathbf{disc}(G(t,y))$. Thus, $C_{\alpha\beta} = F(y_0)$ and $F(y)$ has degree $\delta_A^4\delta_B^2$. We may compute y_0 to be the smallest positive integer such that $F(y_0) \neq 0$. For the best case, this will takes $O(\delta_A^6\delta_B^3)$ arithmetic operations; for the worest case, it takes $O(\delta_A^{10}\delta_B^5)$ arithmetic operations since $F(y)$ has $\delta_A^4\delta_B^2$ roots. If we choose y_0 to be the smallest integer such that $y_0 > 1 + C_{\max}$, then $F(y_0) \neq 0$ since $1 + C_{\max}$ is the root bound of $F(y)$. But, in this case, $C_{\alpha\beta} = F(y_0)$ may be very large.

To analyze the binary length of $C_{\alpha\beta}$, we need the following theorem which is a generation of the result of Goldstein and Graham [4].

Theorem 2 *Let* $A(x_1, x_2, \ldots, x_z) = (A_{\iota\kappa}(x_1, x_2, \ldots, x_z))$ *be a* $n \times n$ *matrix whose elements are polynomials and let* $\det(A(x_1, x_2, \ldots, x_z)) = \sum_{\mu_z}(\cdots(\sum_{\mu_2}(\sum_{\mu_1} a_{\mu_1\mu_2\cdots\mu_z}x_1^{\mu_1})x_2^{\mu_2})\cdots)x_z^{\mu_z}$. *If* $w_{\iota\kappa}$ *denotes the sum of the absolute values of the coefficients of* $A_{\iota\kappa}(x_1, x_2, \ldots, x_z)$ *then*

$$\left(\sum_{\mu_z}\cdots\sum_{\mu_2}\sum_{\mu_1}|a_{\mu_1\mu_2\cdots\mu_z}|^2\right)^{1/2} \leq \left(\prod_{\iota=1}^{n}\sum_{j=1}^{n}w_{\iota\kappa}^2\right)^{1/2}$$

Proof. Since $|A_{i\kappa}(e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_s})| \leq w_{i\kappa}$, it follows from Hadamard's inequality that

$$|\det(A(e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_s}))|^2 \leq \prod_{i=1}^{n}\sum_{\kappa=1}^{n} |A_{i,\kappa}(e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_s})|^2 \leq \prod_{i=1}^{n}\sum_{\kappa=1}^{n} w_{i\kappa}^2.$$

However,

$$\begin{aligned}
&\frac{1}{(2\pi)^s}\int_0^{2\pi}\int_0^{2\pi}\cdots\int_0^{2\pi} |\det(A(e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_s}))|^2\, d\theta_s \cdots d\theta_2\, d\theta_1 \\
&= \frac{1}{2\pi}\int_0^{2\pi}\frac{1}{2\pi}\int_0^{2\pi}\cdots\frac{1}{2\pi}\int_0^{2\pi}\Big(\sum_{\mu_s}\cdots\Big(\sum_{\mu_2}\Big(\sum_{\mu_1} a_{\mu_1\mu_2\cdots\mu_s}e^{i\mu_1\theta_1}\Big)e^{i\mu_2\theta_2}\Big)\cdots e^{i\mu_s\theta_s}\Big) \\
&\quad \Big(\sum_{\mu_s}\cdots\Big(\sum_{\mu_2}\Big(\sum_{\mu_1} \bar{a}_{\mu_1\mu_2\cdots\mu_s}e^{-i\mu_1\theta_1}\Big)e^{-i\mu_2\theta_2}\Big)\cdots e^{-i\mu_s\theta_s}\Big)\, d\theta_s \cdots d\theta_2\, d\theta_1 \\
&= \sum_{\mu_s}\cdots\sum_{\mu_3}\frac{1}{2\pi}\int_0^{2\pi}\frac{1}{2\pi}\int_0^{2\pi}\Big(\sum_{\mu_2}\Big(\sum_{\mu_1} a_{\mu_1\mu_2\cdots\mu_s}e^{i\mu_1\theta_1}\Big)e^{i\mu_2\theta_2}\Big) \\
&\quad \Big(\sum_{\mu_2}\Big(\sum_{\mu_1} \bar{a}_{\mu_1\mu_2\cdots\mu_s}e^{-i\mu_1\theta_1}\Big)e^{-i\mu_2\theta_2}\Big)\, d\theta_2\, d\theta_1 \\
&= \sum_{\mu_s}\cdots\sum_{\mu_2}\frac{1}{2\pi}\int_0^{2\pi}\Big(\sum_{\mu_1} a_{\mu_1\mu_2\cdots\mu_s}e^{i\mu_1\theta_1}\Big)\Big(\sum_{\mu_1} \bar{a}_{\mu_1\mu_2\cdots\mu_s}e^{-i\mu_1\theta_1}\Big)\, d\theta_1 \\
&= \sum_{\mu_s}\cdots\sum_{\mu_2}\sum_{\mu_1} |a_{\mu_1\mu_2\cdots\mu_s}|^2
\end{aligned}$$

Hence,

$$\begin{aligned}
&\sum_{\mu_s}\cdots\sum_{\mu_2}\sum_{\mu_1} |a_{\mu_1\mu_2\cdots\mu_s}|^2 \\
&\quad = \frac{1}{(2\pi)^s}\int_0^{2\pi}\int_0^{2\pi}\cdots\int_0^{2\pi} |\det(A(e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_s}))|^2\, d\theta_s \cdots d\theta_2\, d\theta_1 \\
&\quad \leq \frac{1}{(2\pi)^s}\int_0^{2\pi}\int_0^{2\pi}\cdots\int_0^{2\pi} \prod_{i=1}^{n}\sum_{\kappa=1}^{n} w_{i\kappa}^2\, d\theta_s \cdots d\theta_2\, d\theta_1 \\
&\quad = \prod_{i=1}^{n}\sum_{\kappa=1}^{n} w_{i\kappa}^2 \qquad \square
\end{aligned}$$

Corollary 3 *Suppose $A(x,y) = (A_{ij}(x,y))$ be a $n \times n$ matrix whose elements are polynomials and let $a_0, a_1, \cdots, a_m$ be the coefficients of the polynomial representation of $\det(A(x,y))$. If w_{ij} denotes the sum of the absolute values of the coefficients of $A_{ij}(x,y)$ then*

$$\Big(\sum_{k=0}^{m} |a_k|^2\Big)^{1/2} \leq \left(\prod_{i=1}^{n}\sum_{j=1}^{n} w_{ij}^2\right)^{1/2}$$

By Corollary 3, we have $\|\hat{B}\|_2 \leq \|A\|_2^{\delta_A}(\delta_A^{1/2}\delta_B B_{\max})^{\delta_A}$. If $A(t) = \sum_{j=0}^{\delta_A} a_j t^j$, then

$$A(t - y_0 u) = \sum_{j=0}^{\delta_A} \left(\sum_{i=j}^{\delta_A} a_i \binom{i}{j} t^{i-j} y_0^j \right) u^j .$$

Hence, by Corollary 3, $\|G(t, y_0)\|_2 \leq K^{\delta_A \delta_B} \|\hat{B}\|_2^{\delta_A}$, where

$$K = \sqrt{\sum_{j=0}^{\delta_A} \left(\sum_{i=j}^{\delta_A} a_i \binom{i}{j} y_0^j \right)^2} \leq A_{\max} y_0^{\delta_A} 2^{\delta_A}.$$

But, $C_{\alpha\beta} = |F(y_0)| \leq \|G(t, y_0)\|_2^{\delta_A^2 \delta_B}$. Hence the binary length of $C_{\alpha\beta}$ is

$$O(\delta_A^4 \delta_B^2 \log(2y_0) + (\delta_A^3 \delta_B^2 + \delta_A^4 \delta_B) \log A_{\max} + \delta_A^4 \delta_B \log B_{\max}).$$

3 Double Extensions

Definition. Let $\mathcal{R}$ be a ring and χ an element of some field $\mathbf{F}$ containing $\mathcal{R}$. We shall say that χ is *integral* over $\mathcal{R}$, or for short $\mathcal{R}$-*integral*, if the element χ satisfies an equation

$$\chi^n + a_{n-1}\chi^{n-1} + \cdots + a_0 = 0$$

with coefficients $a_i \in \mathcal{R}$, and an integer $n \geq 1$. χ is said to be integral of degree n over $\mathcal{R}$ if χ doesn't satisfy any nonzero monic polynomial over $\mathcal{R}$ of degree less than n.

Let $A, B, \alpha, \beta, C_\alpha, \mathcal{R}_\alpha$ be as in section 1. Obviously, β is $\mathbf{Z}[\alpha]$-integral. Let $\zeta \in \mathcal{R}_{\alpha\beta}$. Then ζ is also $\mathbf{Z}[\alpha]$-integral since ζ is $\mathbf{Z}$-integral. We may find $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\delta_B} \in \mathbf{Z}[\alpha]$ and an integer $e \neq 0$ such that regarding each ε_i as a polynomial in α over the integers we have no common factor amongst all the coefficients of these polynomials and

$$\zeta = (\varepsilon_1 \beta^0 + \cdots + \varepsilon_{\delta_B} \beta^{\delta_B - 1})/e.$$

Suppose $\beta_1, \ldots, \beta_{\delta_B}$ are all the roots of B. Let

$$\zeta_j = (\varepsilon_1 \beta_j^0 + \cdots + \varepsilon_{\delta_B} \beta_j^{\delta_B - 1})/e$$

for $j = 1, 2, \ldots, \delta_B$. The last system of equations may be considered as a system of equations in $\varepsilon_i e^{-1} \in \mathbf{Q}(\alpha)$ for $i = 1, \ldots, \delta_B$. If we denote its determinant by Δ, then $\Delta^2 = \mathbf{disc}(B)$. Since $\mathbf{disc}(B) \in \mathbf{Z}[\alpha]$, Δ is integral over $\mathbf{Z}[\alpha]$, not necessarily lying in the field $\mathbf{Q}(\alpha)(\beta)$. But Cramer's rule shows that the numbers $\Upsilon_i = \Delta\varepsilon_i e^{-1}$ are integral over $\mathbf{Z}[\alpha]$ since both β and ζ are integral over $\mathbf{Z}[\alpha]$; thus $\Delta\Upsilon_i$ are also integral over $\mathbf{Z}[\alpha]$. But $\Delta\Upsilon_i = \Delta^2\varepsilon_i e^{-1} = \mathbf{disc}(B)\varepsilon_i e^{-1}$ are in $\mathbf{Q}(\alpha)$; so that $\Delta\Upsilon_i$ are in $\mathcal{R}_\alpha$; hence $\Delta\Upsilon_i \in \frac{1}{C_\alpha}\mathbf{Z}[\alpha]$. It follows that e divides all the numbers $C_\alpha\Delta^2\varepsilon_i$ for $i = 1, \ldots, \delta_B$. Although we have no common factor amongst all the coefficients of ε_i $(i = 1, \ldots, \delta_B)$, it does not follow that e divides $C_\alpha\Delta^2$. When multiplied by ε_i, Δ^2 could produce a common factor in the coefficients even though neither Δ^2 nor ε_i had any common factor in their coefficients.

Example 1 Suppose $A(t) = t^2 + 2t + 2$. Then, $\alpha^2 + 2\alpha + 2 = 0$. If $\Delta^2 = \alpha + 4$ and $\varepsilon_i = 3\alpha + 2$, then either Δ^2 nor ε_i had any common factor in their coefficients. But $\Delta^2 \cdot \varepsilon_i = (\alpha + 4)(3\alpha + 2) = 8\alpha + 2$ which is divided by 2.

Let $\Gamma = \sum_{j=0}^{\delta_A - 1} c_j \alpha^j \in \mathbf{Z}[\alpha]$. Define a map $\phi : \mathbf{Z}[\alpha] \to \mathbf{Z}[t]$ by

$$\phi(\Gamma) = \sum_{j=0}^{\delta_A - 1} c_j t^j.$$

Let F be the image of Δ^2 under ϕ and let $F(t) = w \cdot G(t)$ where $G(t)$ is the primitive part of $F(t)$. Clearly, w is the content of $F(t)$. We will show that e divides $C_\alpha \cdot w \cdot \mathbf{res}(A, G)$.

Theorem 4 *Suppose $G(t), A(t) \in \mathbf{Z}[t]$ are two primitive polynomials in t and suppose $A(t)$ is monic and $\delta_G < \delta_A$. Let $E(t) \in \mathbf{Z}[t]$ be an arbitrary primitive polynomial with $\delta_E < \delta_A$. If an integer c divides the remainder of $G(t)E(t)$ divided by $A(t)$, then c divides* $\mathbf{res}(A, G)$.

Proof. Let $F(t)$ be the remainder of $G(t)E(t)$ divided by $A(t)$. For convenience' sake, we need the following definitions. Let $A_i(x) \in \mathbf{Z}[x]$ $(i = 1, \ldots, m)$ be polynomials and let $\delta_{A_i} < m$. Then $\mathbf{mat}(A_1, A_2, \ldots, A_m)$ denotes the $m \times m$ matrix whose $(i, m - j)$th entry is the coefficient of x^j in $A_i(x)$. We denote by $\mathbf{det}(A_1, A_2, \ldots, A_m)$ the determinant of $\mathbf{mat}(A_1, A_2, \ldots, A_m)$.

Then, we can write

$$\mathbf{res}(A,G) = \mathbf{det}(x^{\delta_G-1}A, x^{\delta_G-2}A, \ldots, A, x^{\delta_A-1}G, x^{\delta_A-2}G, \ldots, G).$$

Let $E(t) = \sum_{i=0}^{\delta_E} e_i t^i$. We have, for $i = 0, 1, \ldots, \delta_E$,

$$\begin{aligned} e_i \cdot \mathbf{res}(A,G) &= e_i \cdot \mathbf{det}(x^{\delta_G-1}A, x^{\delta_G-2}A, \ldots, A, x^{\delta_A-1}G, x^{\delta_A-2}G, \ldots, G) \\ &= \mathbf{det}(x^{\delta_G-1}A, x^{\delta_G-2}A, \ldots, A, x^{\delta_A-1}G, \ldots, e_i x^i G, \ldots, G) \end{aligned}$$

For all $j \neq i$, $0 \leq j \leq \delta_E$, adding the $(m-i)$th row by the product of e_j and the $(m-j)$th row, we have

$$e_i \cdot \mathbf{res}(A,G) = \mathbf{det}(x^{\delta_G-1}A, x^{\delta_G-2}A, \ldots, A, x^{\delta_A-1}G, \ldots, x^{i+1}G, GE, x^{i-1}G, \ldots, G).$$

For $j = 1, \ldots, \delta_G$, subtracting the $(m-i)$th row by a multiple of the jth row such that the sequence of row operations correspond to the long-division of $G(t)E(t)$ by $A(t)$, we eventually reduce $e_i \cdot \mathbf{res}(A,G)$ to

$$e_i \cdot \mathbf{res}(A,G) = \mathbf{det}(x^{\delta_G-1}A, x^{\delta_G-2}A, \ldots, A, x^{\delta_A-1}G, \ldots, x^{i+1}G, F, x^{i-1}G, \ldots, G).$$

If c divides $F(t)$, then clearly c divides all the $e_i \cdot \mathbf{res}(A,G)$, for $i = 0, 1, \ldots, \delta_E$. But, $E(t)$ is a primitive polynomial so that e_i $(i = 0, 1, \ldots, \delta_E)$ don't have common factors. It follows that c divides $\mathbf{res}(A,G)$. □

Theorem 4 implies that e divides $C_\alpha \cdot w \cdot \mathbf{res}(A,G)$. Let $C_\beta = w \cdot \mathbf{res}(A,G)$. We obtain e divides $C_\alpha C_\beta$ and

$$\zeta \cdot C_\alpha \cdot C_\beta = (C_\alpha \cdot C_\beta \cdot e^{-1})(\varepsilon_1 \beta^0 + \cdots + \varepsilon_{\delta_B} \beta^{\delta_B - 1}) \in \mathbf{Z}[\alpha][\beta].$$

Hence, $\mathcal{R}_{\alpha\beta} \subseteq \dfrac{1}{C_\alpha C_\beta}\mathbf{Z}[\alpha][\beta]$. We have shown the following theorem.

Theorem 5 *Suppose F is the image of $\mathbf{disc}(B)$ under ϕ and let $F(t) = w \cdot G(t)$ where $G(t)$ is the primitive part of $F(t)$. If $C_\alpha = \mathbf{disc}(A)$ and $C_\beta = w \cdot \mathbf{res}(A(t), G(t))$, then $\mathcal{R}_{\alpha\beta} \subseteq \dfrac{1}{C_\alpha C_\beta}\mathbf{Z}[\alpha][\beta]$.*

It takes $O(\delta_B^3)$ arithmetic steps in $\mathbf{Z}[\alpha]$ to compute $\mathrm{disc}(B)$. But, to perform one arithmetic step in $\mathbf{Z}[\alpha]$ needs $O(\delta_A \log \delta_A)$ integer arithmetic operations. Thus, to compute $\mathrm{disc}(B)$ takes integer arithmetic operations $O(\delta_B^3 \delta_A \log \delta_A)$. And, it takes integer arithmetic operations $O(\delta_A^3)$ to compute $\mathrm{res}(A(t), G(t))$. Hence, The overall arithmetic steps needed for computing C_β is $O(\delta_B^3 \delta_A \log \delta_A + \delta_A^3)$.

By Theorem 2, $|\mathrm{disc}(B)| \leq \delta_B^{\delta_B/2}(B_{\max} A_{\max}^{\delta_A})^{\delta_B}$. Thus, $C_\beta \leq \delta_B^{\delta_B \delta_A}(B_{\max} A_{\max}^{\delta_A})^{\delta_B \delta_A}$. Hence, the binary length of $C_\alpha C_\beta$ is $O(\delta_A \delta_B(\log \delta_B + \delta_A \log A_{\max} + \log B_{\max}))$.

4 Multiple Extensions

In this section, we generalize our result to the filed $\mathbf{Q}(\sigma_1)(\sigma_2)\cdots(\sigma_z)$ where σ_j $(j = 1, \ldots, z)$ are recursively defined as follows:

$$\begin{cases} \sigma_1 \text{ is an algebraic integer} \\ \sigma_j \text{ is integral of degree} \geq 2 \text{ over } \mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_{j-1}]. \end{cases}$$

Let σ_j satisfy a monic irreducible polynomial $S_j(x_j) \in \mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_{j-1}][x_j]$ for $j = 1, \ldots, z$. Suppose $\Gamma = \sum_{\mu_j=0}^{\delta_{S_j}-1} \cdots \sum_{\mu_2=0}^{\delta_{S_2}-1} \sum_{\mu_1=0}^{\delta_{S_1}-1} c_{\mu_1\mu_2\cdots\mu_j} \sigma_1^{\mu_1}\sigma_2^{\mu_2}\cdots\sigma_j^{\mu_j}$. For $j = 1, \ldots, z$, define a map $\phi_j : \mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_{j-1}][\sigma_j] \to \mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_{j-1}][x_j]$ by

$$\phi(\Gamma) = \sum_{\mu_j=0}^{\delta_{S_j}-1} \cdots \sum_{\mu_2=0}^{\delta_{S_2}-1} \sum_{\mu_1=0}^{\delta_{S_1}-1} c_{\mu_1\mu_2\cdots\mu_j} \sigma_1^{\mu_1}\sigma_2^{\mu_2}\cdots\sigma_{j-1}^{\mu_{j-1}} x_j^{\mu_j}.$$

We denote by $\mathcal{R}_{\sigma_1\sigma_2\cdots\sigma_s}$ the algebraic integers contained in $\mathbf{Q}(\sigma_1)(\sigma_2)\cdots(\sigma_z)$. Algorithm 1 computes C_{σ_i} $(i = 1, \ldots, z)$ such that

$$\mathcal{R}_{\sigma_1\sigma_2\cdots\sigma_s} \subseteq \frac{1}{C_{\sigma_1} C_{\sigma_2} \cdots C_{\sigma_s}} \mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_z]. \tag{3}$$

The proof of the correctness of (3) is similar to the proof of Theorem 5.

Algorithm 1 *Computing* C_{σ_i}

1. **if** $i = 1$ **then** $\{C_{\sigma_i} := \mathbf{disc}(S_i)$; **goto** 6$\}$.
2. Compute $\Psi := \mathbf{disc}(S_i) \in \mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{i-1}]$.
3. When regarding Ψ as a polynomial in $i-1$ indeterminates $\sigma_1, \sigma_2, \ldots, \sigma_{i-1}$, let w is the greatest common divisor of all the integer coefficients of Ψ and let $\Gamma := \Psi/w$.
4. **for** $j := i-1$ **downto** 2 **do**
   (a) Compute $\Psi := \mathbf{res}(S_j(x_j), G(x_j)) \in \mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{j-1}]$, where $G(x_j)$ is the image of Γ under ϕ_j.
   (b) When regarding Ψ as a polynomial in $j-1$ indeterminates $\sigma_1, \sigma_2, \ldots, \sigma_{j-1}$, let d be the greatest common divisor of all the integer coefficients of Ψ and let $\Gamma := \Psi/d$.
   (c) $w := w \cdot d$.
5. $C_{\sigma_i} := w \cdot \mathbf{res}(S_1(x_1), G(x_1))$ where $G(x_j)$ is the image of Γ under ϕ_1.
6. **End Algorithm.**

For convenience' sake, we rename variable Ψ and G and d in step 4 to be Ψ_{j-1} and G_j and d_{j-1} respectively and variable Γ in step 4 (a) to be Γ_j. Clearly, variable Γ in step 4 (b) should be changed to Γ_{j-1}; and variables Γ and G in step 5 should be changed to Γ_1 and G_1 respectively. Also, we rename variable Ψ in step 2 & 3 to be Ψ_{i-1} and Γ in step 3 to be Γ_{i-1}. Figure 1 shows the algorithm with renamed variables. Let Γ_j, Ψ_j, G_j and d_j be as in Algorithm 2. We show the following lemma.

Algorithm 2 *Computing* C_{σ_i}.

1. **if** $i = 1$ **then** $\{C_{\sigma_i} := \mathbf{disc}(S_i)$; **goto** $6\}$.
2. Compute $\Psi_{i-1} := \mathbf{disc}(S_i) \in \mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_{i-1}]$.
3. When regarding Ψ_{i-1} as a polynomial in $i-1$ indeterminates $\sigma_1, \sigma_2, \ldots, \sigma_{i-1}$, let w is the greatest common divisor of all the integer coefficients of Ψ_{i-1} and let $\Gamma_{i-1} := \Psi_{i-1}/w$.
4. **for** $j := i-1$ **downto** 2 **do**
   (a) Compute $\Psi_{j-1} := \mathbf{res}(S_j(x_j), G_j(x_j)) \in \mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_{j-1}]$, where $G_j(x_j)$ is the image of Γ_j under ϕ_j.
   (b) When we regard Ψ_{j-1} as a polynomial in $j-1$ indeterminates $\sigma_1, \sigma_2, \ldots, \sigma_{j-1}$, let d_{j-1} be the greatest common divisor of all the integer coefficients of Ψ_{j-1} and let $\Gamma_{j-1} := \Psi_{j-1}/d_{j-1}$.
   (c) $w := w \cdot d_{j-1}$.
5. $C_{\sigma_i} := w \cdot \mathbf{res}(S_1(x_1), G_1(x_1))$ where $G_1(x_j)$ is the image of Γ_1 under ϕ_1.
6. **End Algorithm.**

Figure 1: Algorithm for Computing C_{σ_i}.

Lemma 6 *Suppose ε is an arbitrary element in $\mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_j]$ such that regarding ε as a polynomial in $\sigma_1, \sigma_2, \ldots, \sigma_j$ we have no common factor amongst all the integer coefficients of ε. For $1 \leq j < i$, if an integer e divides all the integer coefficients of $\Gamma_j \cdot \varepsilon$ when $\Gamma_j \cdot \varepsilon$ is regarded as a polynomial in $\sigma_1, \sigma_2, \ldots, \sigma_j$, then e divides $d_1 \cdot d_2 \cdots d_{j-1} \cdot \mathbf{res}(S_1(x_1), G_1(x_1))$.*

Proof. We prove by induction on j.

Basis: If $j = 1$, then this lemma is equivalent to Theorem 4.

Inductive steps: Suppose $2 \leq j < i$. Let $E(x_j)$ be the image of ε under ϕ_j and let $F(x_j)$ be the remainder of $G_j(x_j)E(x_j)$ divided by $S_j(x_j)$. Clearly, $F(\sigma_j) = \Gamma_j \cdot \varepsilon$. Then, we can write

$$\mathbf{res}(S_j, G_j) = \mathbf{det}(x^{\delta_{G_j}-1}S_j, x^{\delta_{G_j}-2}S_j, \ldots, S_j, x^{\delta_{S_j}-1}G_j, x^{\delta_{S_j}-2}G_j, \ldots, G_j).$$

Let $E(x_j) = \sum_{k=0}^{\delta_E} \varepsilon_k x_j^k$. We have, for $k = 0, 1, \ldots, \delta_E$,

$$\begin{aligned}\varepsilon_k \cdot \mathbf{res}(S_j, G_j) &= \varepsilon_k \cdot \mathbf{det}(x^{\delta_{G_j}-1}S_j, x^{\delta_{G_j}-2}S_j, \ldots, S_j, x^{\delta_{S_j}-1}G_j, x^{\delta_{S_j}-2}G_j, \ldots, G_j) \\ &= \mathbf{det}(x^{\delta_{G_j}-1}S_j, x^{\delta_{G_j}-2}S_j, \ldots, S_j, x^{\delta_{S_j}-1}G_j, \ldots, \varepsilon_k x^k G_j, \ldots, G_j)\end{aligned}$$

For all $l \neq k$, $0 \leq l \leq \delta_E$, adding the $(m-k)$th row by the product of ε_l and the $(m-l)$th row, we have

$$\varepsilon_k \cdot \mathbf{res}(S_j, G_j) = \mathbf{det}(x^{\delta_{G_j}-1}S_j, x^{\delta_{G_j}-2}S_j, \ldots, S_j, x^{\delta_{S_j}-1}G_j, \ldots, x^{k+1}G_j, G_jE, x^{k-1}G_j, \ldots, G_j).$$

For $l = 1, \ldots, \delta_{G_j}$, subtracting the $(m-k)$th row by a multiple of the lth row such that the sequence of row operations correspond to the long-division of $G_j(x_j)E(x_j)$ by $S_j(x_j)$, we eventually reduce $\varepsilon_k \cdot \mathbf{res}(S_j, G_j)$ to

$$\varepsilon_k \cdot \mathbf{res}(S_j, G_j) = \mathbf{det}(x^{\delta_{G_j}-1}S_j, x^{\delta_{G_j}-2}S_j, \ldots, S_j, x^{\delta_{S_j}-1}G_j, \ldots, x^{k+1}G_j, F, x^{k-1}G_j, \ldots, G_j).$$

When we regard $\sigma_1, \sigma_2, \ldots, \sigma_j$ as indeterminates, if e divides $\Gamma_j \cdot \varepsilon$, then e divides $F(x_j)$, so that e divides all the $\varepsilon_k \cdot \mathbf{res}(S_j, G_j)$, for $k = 0, 1, \ldots, \delta_E$. Thus, according to Algorithm 2, e divides all

the $\varepsilon_k \cdot d_{j-1} \cdot \Gamma_{j-1} = d_{j-1} \cdot \varepsilon_k \cdot \Gamma_{j-1}$. When we regard $\sigma_1, \sigma_2, \ldots, \sigma_j$ as indeterminates, let c_k be the greatest common divisor of all the integer coefficients of ε_k and let $\epsilon_k = \varepsilon_k / c_k$ for $k = 0, 1, \ldots, \delta_E$. Thus e divides all the $d_{j-1} \cdot c_k \cdot \epsilon_k \cdot \Gamma_{j-1}$ when we regard $\sigma_1, \sigma_2, \ldots, \sigma_j$ as indeterminates. By the inductive hypothesis, we have e divides all the $d_{j-1} \cdot c_k \cdot d_1 \cdot d_2 \cdots d_{j-2} \cdot \mathrm{res}(S_1(x_1), G_1(x_1))$ for $i = 1, 2, \ldots, m$. But, c_k $(l = 0, 1, \ldots, m)$ don't have common factors since regarding ε as a polynomial in $\sigma_1, \sigma_2, \ldots, \sigma_j$ we have no common factor amongst all the integer coefficients of ε. It follows that e divides $d_1 \cdot d_2 \cdots d_{j-1} \cdot \mathrm{res}(S_1(x_1), G_1(x_1))$. □

Proof of the correctness of (3). We prove by induction on z.

Basis: If $z = 1$, then (3) is equivalent to Lemma 1. If $z = 2$, then (3) is equivalent to Theorem 5.

Inductive steps: Let $\zeta \in \mathcal{R}_{\sigma_1 \sigma_2 \cdots \sigma_z}$. Then ζ is $\mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{z-1}]$-integral since ζ is $\mathbf{Z}$-integral. We may find $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\delta_{S_z}} \in \mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{z-1}]$ and an integer $e \neq 0$ such that regarding each ε_i as a polynomial in $\sigma_1 \sigma_2 \cdots \sigma_{z-1}$ over the integers we have no common factor amongst all the coefficients of these polynomials and

$$\zeta = (\varepsilon_1 \sigma_z^0 + \cdots + \varepsilon_{\delta_{S_z}} \sigma_z^{\delta_{S_z}-1})/e.$$

Suppose $\sigma_{z,1}, \ldots, \sigma_{z,\delta_{S_z}}$ are all the roots of S_z. Let

$$\zeta_j = (\varepsilon_1 \sigma_{z,j}^0 + \cdots + \varepsilon_{\delta_{S_z}} \sigma_{z,j}^{\delta_{S_z}-1})/e$$

for $j = 1, 2, \ldots, \delta_{S_z}$. The last system of equations may be considered as a system of equations in $\varepsilon_i e^{-1} \in \mathbf{Q}(\sigma_1)(\sigma_2) \cdots (\sigma_{z-1})$ for $i = 1, \ldots, \delta_{S_z}$. If we denote its determinant by Δ, then $\Delta^2 = \mathrm{disc}(S_z)$. Since $\mathrm{disc}(S_z) \in \mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{z-1}]$, Δ is integral over $\mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{z-1}]$, not necessarily lying in the field $\mathbf{Q}(\sigma_1)(\sigma_2) \cdots (\sigma_z)$. But Cramer's rule shows that the numbers $\Upsilon_i = \Delta \varepsilon_i e^{-1}$ are integral over $\mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{z-1}]$ since both σ_z and ζ are integral over $\mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{z-1}]$; thus $\Delta \Upsilon_i$ are also integral over $\mathbf{Z}[\sigma_1][\sigma_2] \cdots [\sigma_{z-1}]$. But $\Delta \Upsilon_i = \Delta^2 \varepsilon_i e^{-1} = \mathrm{disc}(S_z) \varepsilon_i e^{-1}$ are in $\mathbf{Q}(\sigma_1)(\sigma_2) \cdots (\sigma_{z-1})$; so that $\Delta \Upsilon_i$ are in $\mathcal{R}_{\sigma_1 \sigma_2 \cdots \sigma_{z-1}}$; hence, by inductive hypothesis, $\Delta \Upsilon_i \in$

$\frac{1}{C_{\sigma_1}C_{\sigma_2}\cdots C_{\sigma_{z-1}}}\mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_{z-1}]$. It follows that e divides all the numbers $C_{\sigma_1}C_{\sigma_2}\cdots C_{\sigma_{i-1}}\Delta^2\varepsilon_i$ for $i = 1,\ldots,\delta_{S_i}$, when we regard $\sigma_1,\sigma_2,\ldots,\sigma_j$ as indeterminates. In Algorithm 2, $\Psi_{z-1} = \Delta^2$ and $w\cdot\Gamma_{z-1} = \Psi_{z-1}$; so that e divides all the numbers $C_{\sigma_1}C_{\sigma_2}\cdots C_{\sigma_{i-1}}\cdot w\cdot\Gamma_{z-1}\cdot\varepsilon_i$ for $i = 1,\ldots,\delta_{S_i}$, when we regard $\sigma_1,\sigma_2,\ldots,\sigma_j$ as indeterminates. But, by Lemma 6, we have that e divides $C_{\sigma_1}C_{\sigma_2}\cdots C_{\sigma_{i-1}}\cdot w\cdot d_1\cdot d_2\cdots d_{z-2}\cdot\mathrm{res}(S_1(x_1),G(x_1))$. From Algorithm 2, we know that $C_{\sigma_i} = w\cdot d_1\cdot d_2\cdots d_{z-2}\cdot\mathrm{res}(S_1(x_1),G(x_1))$. Thus, e divides $C_{\sigma_1}C_{\sigma_2}\cdots C_{\sigma_i}$ and

$$\zeta\cdot C_{\sigma_1}C_{\sigma_2}\cdots C_{\sigma_i} = (C_{\sigma_1}C_{\sigma_2}\cdots C_{\sigma_i}\cdot e^{-1})(\varepsilon_1\sigma_z^0+\cdots+\varepsilon_{\delta_{S_i}}\sigma_z^{\delta_{S_i}-1})\in\mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_z].$$

Hence, $\mathcal{R}_{\sigma_1\sigma_2\cdots\sigma_i}\subseteq\frac{1}{C_{\sigma_1}C_{\sigma_2}\cdots C_{\sigma_i}}\mathbf{Z}[\sigma_1][\sigma_2]\cdots[\sigma_z]$. □

5 Factoring Polynomials over Algebraic Number Fields

We'll present an application of Algorithm 1. Let us consider the factorization of monic squarefree polynomials over algebraic number field $\mathbf{Q}(\sigma_1)(\sigma_2)\cdots(\sigma_z)$, where σ_j $(j = 1,\ldots,z)$ are as in section 1 (2). In this section, we discuss the case of $z = 2$. It is easy to extend the case of $z = 2$ to the general case.

Let $A, B, \alpha, \beta, C_\alpha, C_\beta, \mathcal{R}_{\alpha\beta}$ be as in section 3. Let $f\in\mathbf{Q}(\alpha)(\beta)[x]$ be a *monic squarefree* polynomial. Then we can write $f\in\frac{1}{d}\mathbf{Z}[\alpha][\beta][x]$. We want to choose a positive integer D such that f and all the monic factors of f in $\mathbf{Q}(\alpha)(\beta)[x]$ are in $\frac{1}{D}\mathbf{Z}[\alpha][\beta][x]$. The following lemma has been shown by Weinberger and Rothschild [8]:

Lemma 7 (Weinberger and Rothschild) *Let $g(x)\in\frac{1}{d}\mathcal{R}_{\alpha\beta}[x]$ be monic, and suppose $g(x) = v(x)w(x)\in\mathbf{Q}(\alpha)(\beta)$, where $v(x), w(x)$ are monic. Then $v(x), w(x)\in\frac{1}{d}\mathcal{R}_{\alpha\beta}[x]$.*

Since $\mathbf{Z}[\alpha][\beta]\subseteq\mathcal{R}_{\alpha\beta}$, we have $f(x)\in\frac{1}{d}\mathcal{R}_{\alpha\beta}[x]$. Hence, by Lemma 7, the monic factors of $f(x)$ will also be in $\frac{1}{d}\mathcal{R}_{\alpha\beta}[x]$. Thus, by (1), the monic factors of $f(x)$ will be in $\frac{1}{dC_\alpha C_\beta}\mathbf{Z}[\alpha][\beta][x]$.

Therefore, we can take

$$D = d \cdot C_\alpha \cdot C_\beta$$

such that f and all the monic factors of f in $\mathbf{Q}(\alpha)(\beta)[x]$ are in $\frac{1}{D}\mathbf{Z}[\alpha][\beta][x]$.

The remainder of this section is similar to [6]. We choose p as a prime number such that

$$p \text{ does not divide } D \cdot \mathbf{disc}(A) \cdot \mathbf{disc}(B) \cdot \mathbf{res}(f, f'),$$

Let k be some positive integer. We denote by $\mathbf{Z}_p$ the field of integers modulo p and by $\mathbf{Z}_{p^k}$ the ring of integers modulo p^k. Since p and D are relatively prime, for any $c \in \frac{1}{D}\mathbf{Z}$, ($c$ modulo p) and (c modulo p^k) exist. For $F = \sum_i c_i t^i \in \frac{1}{D}\mathbf{Z}[t]$ we denote the polynomial $\sum_i (c_i \text{ modulo } p^k) t^i \in \mathbf{Z}_{p^k}[t]$ by $F_{/p^k}$ and denote the polynomial $\sum_i (c_i \text{ modulo } p) t^i \in \mathbf{Z}_p[t]$ by $F_{/p}$.

Using Hensel's Lemma and Berlekamp's algorithm [1] for factoring over finite fileds, we can construct a polynomial $H \in \mathbf{Z}[t]$ such that H satisfies the following conditions:

$$H \text{ is monic,} \tag{4}$$

$$H_{/p^k} \text{ divides } A_{/p^k} \text{ in } \mathbf{Z}_{p^k}[t], \tag{5}$$

$$H_{/p} \text{ is irreducible in } \mathbf{Z}_p[t], \tag{6}$$

$$(H_{/p})^2 \text{ does not divide } A_{/p} \text{ in } \mathbf{Z}_p[t] \tag{7}$$

We denote by $\mathbf{Z}^t_{p,H}$ the finite field $\mathbf{Z}_p[t]/(H_{/p})$ and by $\mathbf{Z}^t_{p^k,H}$ the ring $\mathbf{Z}_{p^k}[t]/(H_{/p^k})$. For $F = \sum_i F_i(t)u^i \in \frac{1}{D}\mathbf{Z}[t][u]$ we denote by $F_{/p,H}$ the polynomial $\sum_i (F_{i/p} \text{ modulo } H_{/p}) u^i \in \mathbf{Z}^t_{p,H}[u]$ and by $F_{/p^k,H}$ the polynomial $\sum_i (F_{i/p^k} \text{ modulo } H_{/p^k}) u^i \in \mathbf{Z}^t_{p^k,H}[u]$. Note that the working ring of each modulo operation depends on its operands.

By Hensel's Lemma and Berlekamp's algorithm [2], we can also construct a polynomial $\Xi \in \mathbf{Z}[\alpha][u]$ such that Ξ satisfies the following conditions:

$$\Xi \text{ is monic,} \tag{8}$$

$$\Xi_{/p^k,H} \text{ divides } B_{/p^k,H} \text{ in } \mathbf{Z}^t_{p^k,H}[u], \tag{9}$$

$$\Xi_{/p,H} \text{ is irreducible in } \mathbf{Z}^t_{p,H}[u], \tag{10}$$

$$(\Xi_{/p,H})^2 \text{ does not divide } B_{/p,H} \text{ in } \mathbf{Z}^t_{p,H}[u] \tag{11}$$

We denote by $\mathbf{Z}^{tu}_{p,H,\Xi}$ the finite field $\mathbf{Z}^t_{p,H}[u]/(\Xi_{/p,H})$ and by $\mathbf{Z}^{tu}_{p^k,H,\Xi}$ the ring $\mathbf{Z}^t_{p^k,H}[u]/(\Xi_{/p^k,H})$. For $F = \sum_i F_i(t,u)x^i \in \frac{1}{D}\mathbf{Z}[t][u][x]$ we denote by $F_{/p,H,\Xi}$ the polynomial $\sum_i (F_{i/p,H} \text{ modulo } \Xi_{/p,H})x^i \in \mathbf{Z}^{tu}_{p,H,\Xi}[x]$ and by $F_{/p^k,H,\Xi}$ the polynomial $\sum_i (F_{i/p^k,H} \text{ modulo } \Xi_{/p^k,H})x^i \in \mathbf{Z}^{tu}_{p^k,H,\Xi}[x]$.

Again, by Hensel's Lemma and Berlekamp's algorithm [2], we construct a monic polynomial $h \in \frac{1}{D}\mathbf{Z}[\alpha][\beta][x]$ such that h satisfies the following conditions:

$$h \text{ is monic,} \tag{12}$$

$$h_{/p^k,H,\Xi} \text{ divides } f_{/p^k,H,\Xi} \text{ in } \mathbf{Z}^{tu}_{p^k,H,\Xi}[x], \tag{13}$$

$$h_{/p,H,\Xi} \text{ is irreducible in } \mathbf{Z}^{tu}_{p,H,\Xi}[x], \tag{14}$$

$$(h_{/p,H,\Xi})^2 \text{ does not divide } f_{/p,H,\Xi} \text{ in } \mathbf{Z}^{tu}_{p,H,\Xi}[x] \tag{15}$$

Let $n = \delta_f$ and $l = \delta_h$ and let m be an integer such that $l \le m < n$. We define L as the collection of polynomials $g \in \frac{1}{D}\mathbf{Z}[\alpha][\beta][x]$ such that: (i) $\delta_g \le m$, (ii) if $\delta_g = m$, then $\mathbf{lead}(g) \in \mathbf{Z}$, where $\mathbf{lead}(g)$ denotes the leading coefficient of g, (iii) $h_{/p^k,H,\Xi}$ divides $g_{/p^k,H,\Xi}$ in $\mathbf{Z}^{tu}_{p^k,H,\Xi}[x]$. We identify such a polynomial

$$g = \sum_{i=0}^{m-1}\sum_{\mu=0}^{\delta_B-1}\sum_{\nu=0}^{\delta_A-1} a_{i\mu\nu}\alpha^\nu\beta^\mu x^i + a_{m00}x^m$$

with the $(m\cdot\delta_B\cdot\delta_A+1)$–dimensional vector $(a_{000}, a_{001}, \ldots, a_{00\delta_A-1}, \ldots, a_{m-1,\delta_B-1,\delta_A-1}, a_{m00})$. We define $|g|$ to be 2-norm of the vector g and define $g_{\max}$ to be ∞-norm of the vector g. It is not difficult to see that L is a lattice in $(\frac{\mathbf{Z}}{D})^{m\delta_B\delta_A+1}$. From the fact that Ξ and H and h are monic, it follows that a basis of L is given by:

$$\{\frac{1}{D}p^k\alpha^\nu\beta^\mu x^i : 0 \le \nu < \delta_H, 0 \le \mu < \delta_\Xi, 0 \le i < l\} \cup$$

$$\{\frac{1}{D}\alpha^{\nu-\delta_H}H(\alpha)\beta^{\mu}x^i : \delta_H \le \nu < \delta_A, 0 \le \mu < \delta_\Xi, 0 \le i < l\} \cup$$

$$\{\frac{1}{D}\alpha^{\nu}\beta^{\mu-\delta_\Xi}\Xi(\beta)x^i : 0 \le \nu < \delta_A, \delta_\Xi \le \mu < \delta_B, 0 \le i < l\} \cup$$

$$\{\frac{1}{D}\alpha^{\nu}\beta^{\mu}hx^{i-l} : 0 \le \nu < \delta_A, 0 \le \mu < \delta_B, l \le i < m\} \cup$$

$$\{hx^{m-l}\}$$

Let $q = m \cdot \delta_B \cdot \delta_A + 1$. We identify the above basis with vectors $b_1, b_2, \ldots, b_q \in (\frac{\mathbf{Z}}{D})^q$. Then $b_1, b_2, \ldots, b_q$ are linearly independent. The following theorem directly follows from A. Lenstra and H. Lenstra and Lovász [7, (1.11), (1.26), (1.37)].

Theorem 8 *Let $N \ge 2$ be an integer such that $|Db_j|^2 \le N$ for $j = 1, 2, \ldots, q$. There is an algorithm, called LLL algorithm, that determines a vector $\tilde{b} \in L$ such that $\tilde{b}$ belongs to a basis of L, and such that $|\tilde{b}|^2 \le 2^{q-1}|\lambda|^2$ for every $\lambda \in L$, $\lambda \ne 0$; the algorithm takes $O(q^4 \log N)$ elementary operations on integers having binary length $O(q \log N)$.*

Let $h_0 \in \frac{1}{D}\mathbf{Z}[\alpha][\beta][x]$ be the unique monic irreducible factor of f such that $h_{/p,H,\Xi}$ divides $h_{0/p,H,\Xi}$ in $\mathbf{Z}^{tu}_{p,H,\Xi}[x]$ and let $\alpha_{\max} = 1 + A_{\max}$ and $\beta_{\max} = 1 + \delta_A B_{\max}\alpha_{\max}^{\delta_A}$. Then, $|\alpha| \le \alpha_{\max}$ and $|\beta| \le \beta_{\max}$. Theorem 9 and Theorem 10 are the generalization of [6, (3.6),(3.11)].

Theorem 9 *Let $b \in L$ satisfy*

$$p^{kl(\delta_H/\delta_A)(\delta_\Xi/\delta_B)} >$$

$$\left(Df_{\max}((n+1)\delta_A\delta_B\alpha_{\max}^{\delta_A-1}\beta_{\max}^{\delta_B-1})^{\frac{1}{2}}\right)^m \left(Db_{\max}((m+1)\delta_A\delta_B\alpha_{\max}^{\delta_A-1}\beta_{\max}^{\delta_B-1})^{\frac{1}{2}}\right)^n. \quad (16)$$

Then b is divisible by h_0 in $\mathbf{Q}[\alpha][\beta][x]$, and in particular $\gcd(f, b) \ne 1$.

Theorem 10 *Suppose that $\tilde{b}$ is as in Theorem 8, and that*

$$p^{kl(\delta_H/\delta_A)(\delta_\Xi/\delta_B)} > \left(Df_{\max}(n+1)^{\frac{1}{2}}\right)^{m+n} \delta_A^{n(\delta_A+1)}\delta_B^{n(\delta_B+1)}$$
$$(\delta_A\delta_B\alpha_{\max}^{\delta_A-1}\beta_{\max}^{\delta_B-1})^{\frac{m}{2}} (2^{m\delta_A\delta_B}\binom{2m}{m}(m+1)\alpha_{\max}^{(\delta_A+1)^2}\beta_{\max}^{(\delta_B+1)^2})^{\frac{n}{2}} \quad (17)$$

Then we have $\delta_h \leq m$ if and only if (16) is satisfied with b replaced by $\tilde{b}$.

In (17), every variable is known except k and m. We calculate the least positive integer k for which (17) holds with m replaced by $n-1$. After k is determined, H, Ξ and h can also be obtained. Note that δ_H and δ_Ξ can be determinated without knowing k. Then we run the following loop:

Loop 1:

For $m = l, l+1, \ldots, n-1$ **do begin**

1. Construct the basis $b_1, b_2, \ldots, b_q$ of the lattice L as described in the beginning of this section, where $q = m \cdot \delta_A \cdot \delta_B + 1$.
2. Apply the LLL algorithm (see Theorem 8) to the basis $b_1, b_2, \ldots, b_q$; and then obtain a vector $\tilde{b}$ belonging to a basis of L such that $|\tilde{b}|^2 \leq 2^{q-1}|\lambda|^2$ for every $\lambda \in L$, $\lambda \neq 0$.
3. **If** (16) is satisfied with b replaced by $\tilde{b}$ **then break.**

end

Suppose, after running the previous procedure, $m = m_0$. If $m_0 \leq n-1$, then a vector $\tilde{b}$ was found. We know from Theorem 10 that $\delta_{h_0} \leq m_0$. Since we try the values $m = l, l+1, \ldots, n-1$ in succession we also know that $\delta_{h_0} > m_0 - 1$, so $\delta_{h_0} = m_0$. By Theorem 9, h_0 divides $\tilde{b}$ in $\mathbf{Q}[\alpha][\beta][x]$ which implies, together with $\delta_{\tilde{b}} \leq m_0$, that $\delta_{\tilde{b}} = m_0$. Since h_0 is monic and, by the definition of lattice L, $\mathrm{lead}(\tilde{b}) \in \mathbf{Z}$, we have $\tilde{b} = c \cdot h_0$, for some constant $c \in \mathbf{Z}$. But $h_0 \in L$ and $\tilde{b}$ belongs to a basis of L. We conclude that $c = \pm 1$, so that $\tilde{b} = \pm h_0$.

If on the other hand $m_0 = n$, then we did not find a vector $\tilde{b}$ satisfying (16). By Theorem 10, $\delta_{h_0} > n-1$; so that $\delta_{h_0} = n$. With h_0 being a factor of f, we have $h_0 = f$.

Now, we know how to compute an irreducible factor of f. The following procedure completely factors a monic squarefree polynomial $f \in \mathbf{Q}[\alpha][\beta][x]$.

procedure *factoring* (f : polynomial);

begin

1. Use the above algorithm to compute an irreducible factor h_0 of f.
2. **if** $f = h_0$ **then return**(h_0) **else** $g := f/h_0$.
3. **return**(h_0 * *factoring*(g)).

end

With Theorem 8, the number of arithmetic operations needed for Procedure factoring is $O(n^6\delta_A^6\delta_B^6 + n^5\delta_A^7\delta_B^5 \log\alpha_{\max} + n^5\delta_A^5\delta_B^7 \log\beta_{\max} + n^5\delta_A^5\delta_B^5 \log(d f_{\max}))$ and the integers on which these operations performed have binary length $O(n^3\delta_A^3\delta_B^3 + n^2\delta_A^4\delta_B^2 \log\alpha_{\max} + n^2\delta_A^2\delta_B^4 \log\beta_{\max} + n^2\delta_A^2\delta_B^2 \log(d f_{\max}))$.

References

[1] E.R. Berlekamp. Factoring polynomials over finite fields. *Bell System Tech. J.*, 46:1853–1859, 1967.

[2] E.R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.*, 24:713–735, 1970.

[3] B. Buchberger, G.E. Collins, and R. Loos. *Computer Algebra.* Spring-Verlag, New York, 2nd edition, 1983.

[4] A.J. Goldstein and R.L. Graham. A hadamard-type bound on the coefficients of a determinant of polynomials. *SIAM Review*, 16:394–395, 1974.

[5] I. N. Herstein. *Topics in Algebra.* Xerox College Publishing, Lexington, Massachusetts, 2nd edition, 1975.

[6] A.K. Lenstra. Factoring polynomials over algebraic number fields. *Proceedings EUROCAL 83 (London) Springer LNCS*, 162:245–254, 1983.

[7] A.K. Lenstra, H.W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[8] P.J. Weinberger and L.P. Rothschild. Factoring polynomials over algebraic number fields. *ACM Transactions on Mathematical Software*, 2:335–350, 1976.

NYU COMPSCI TR-432
Ho, Chung-jen
Multiple extension
algebraic number fields.
c.1